IT-Compliance an Hochschulen

Hans Pongratz
Geschäftsführender Vizepräsident für IT-Systeme & Dienstleistungen
Chief Information Officer

23. November 2012

TUM. Campus

Die TUM in Zahlen

13	Fakultäten	
411	Gebäude	
156	Studiengänge	
~ 32 000	Studierende	32% Studentinnen 16% int. Studierende
478	Professor/-innen	(inkl. Klinika)
~ 9 300	Beschäftigte	
~ 40 000	Alumni	
13	Nobelpreise	
14	Leibniz-Preise	
5	Humboldt Professuren	
#53	2012 Academic Ranking of World Universities (beste dt. Universität)	

Leibniz-Rechenzentrum (LRZ)

- gemeinsames Rechenzentrum LMU, TUM & BAdW
- Hochleistungsrechensysteme für alle bayerischen Hochschulen
- Bundeshöchstleistungsrechner SuperMUC

Dienstekatalog (Auszug):

- Münchner Wissenschaftsnetz (Backbone, LAN & WLAN)
- HPC
- Mail & Groupware, Web, Verzeichnisdienst(e), Storage & Archivierung
- Hosting & Housing, …

=> aber keine Verwaltungs-IT

IT-Goverance

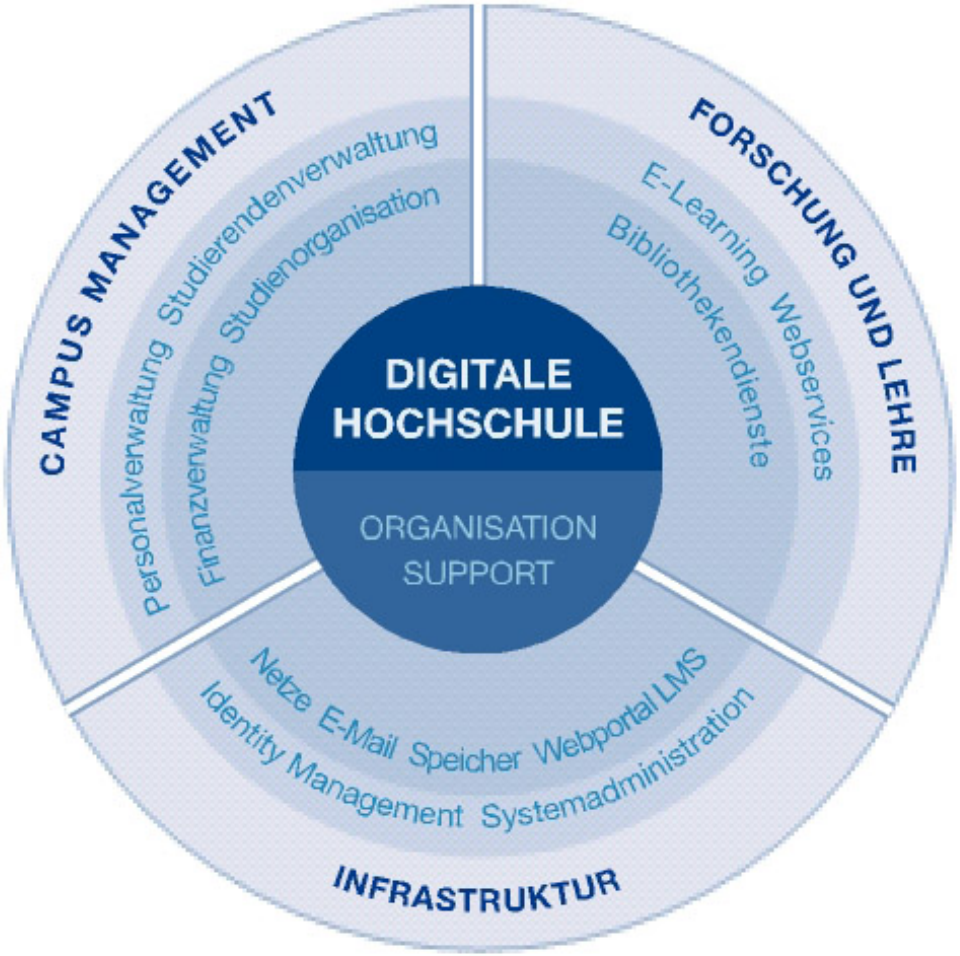
- Rolle des CIO seit Ende 2001 im Rang eines Vizepräsidenten; Wahl durch Hochschulrat auf Vorschlag des Präsidenten und Ressortverantwortung für „IT-Systeme und Dienstleistungen“
- Dekane ernennen Information Officer (IO) für Fakultäten
- Aufgaben des CIO/IO-Gremiums laut Gründungsbeschluss:
  - Schaffung eines Informationsnetzwerks für Support für alle Teile der TUM
  - Vereinheitlichung des Diensteprofils zwischen den Organisationseinheiten (OE)
  - Verbesserung des Wissenstransfers
  - Steigerung der Supportqualität
- Geschäftsordnung regelt Einbindung des CIO bei Beschaffungen

IT-Strategie: Digitale Hochschule

Leitmotiv seit 2002

Abgeschlossene IT-Projekte:

- SAP@TUM
- IntegraTUM
- elecTUM
- mediaTUM
- Data Warehouse
- Corporate Design
- CM@TUM



TUM: Agenda IT

Kernsysteme

- Content Management
- Campus Management
- E-Learning
- Dokumenten- & Publikationsserver
- Personal- & Finanzmanagement
- Data Warehouse
- Verzeichnisdienst
- E-Mail / Groupware
- Netzwerk-Speicher
- Trouble Ticket System
- Evaluationssystem

Strukturen & Management

- CIO/IO-Gremium
- Standort IO-Runden
- ITSZ-Steuerkreis
- ITSZ-Treffen

- Benutzungsrichtlinien
- Passwort-Policy
- Portal-Strategie
- Lieferanten- & Technologiemgmt.
- Meldewesen IT-Sicherheit

Service & Kommunikation

- Dienstleistungskatalog
- Campus Lizenzen
- LS-Starterpaket

- IT- & ITSZ-Newsletter
- Handreichungen
- Schulungen

Infrastruktur

- WLAN-Ausbau
- HPC-Housing
- IP-Telefonie

Projekte

- E-Mail Migration
- elektr. Studierendenakte
- Neugestaltung tum.de
- TUMcard (neue Chipkarte)
- TUMnet (A&C)
- Forschungsdatenmgmt
- Green-IT

Schwarz: produktiv

Blau: in Umsetzung

Rot: geplant

Stand Juni 2012

Ziele IT-Compliance

- Einhalten von Regeln, Gesetze & Vorschriften
- Schadensprävention (auch bzgl. Reputation)
- Sicherstellung rechtskonformen Verhaltens
- Teil der allg. Compliance-Strategie

⇒ **Compliance mit IT-Unterstützung**

&

⇒ **Compliance von IT**

IT ist allerdings Hygienefaktor und Grundlage für Gesamterfolg der Organisation.

Quellen für IT-Compliance Vorgaben

Typ	Beispiele
Gesetze / rechtliche Vorgaben	Bundesdatenschutzgesetz (BDSG) Landesdatenschutzgesetz (BayDSG) Telemediengesetz (TMG) Basel II
Externe Richtlinien / Standards	IT Infrastructure Library (ITIL) ISO 20000 Bayern: Durchführung von IKT-Projekten (BayITR-02) BSI IT-Grundschutz
Interne Richtlinien	Benutzungsrichtlinie Passwort Policy Service Level Agreement (SLA)
Verträge	Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT)

Beispiele für Compliance Vorfälle (1/2)

- **„Programmierer soll Infos über Millionen Griechen gestohlen haben“**
  (20.11.2012, Spiegel online)
- **„Patientendaten offenbar bei Raucherpause verschlampt“**
  (12.10.2012, Die Welt): ca. 300.000 hochsensible Datensätze auf Datenträger vermisst.
- **„Protest gegen Bildungssystem: über 50 Unis gehackt“**
  (4.10.2012, heise online): div. Server von Harvard, Stanford und auch dt. Hochschulen gehackt.
- **„Langfinger im Labor“**
  (2.11.2012, Süddeutsche): Uni-Hausmeister stiehlt jahrelang und verkauft Beute auf ebay.

Beispiele für Compliance Vorfälle (2/2)

- Polizeiliche Anfragen
- Dreiste Phishing Mail 28.8.12:

Ihre Tum E-Mail-Konto für zahlreiche Spam-Aktivitäten von einer ausländischen ip vor kurzem berichtet wurde. Als Ergebnis können Sie nicht in der Lage sein zu empfangen oder zu senden neue E-Mail.
Sie könnten jedoch auch nicht das der Förderung dieser Spam, wie Sie Ihre E-Mail-Konto kompromittiert haben könnten. Um Ihr Konto vor das Versenden von Spam-Mails zu schützen, Sie, Ihre wahre Eigentum an diesem Konto zu bestätigen sind, bitte KLICKEN SIE HIER das Formular ausfüllen und sich erneut an.

Wenn Sie dies tun wird, verletzt die IT Policies.This machen wird Ihr Konto inaktiv.
HINWEIS:! Du wirst ein Passwort-Reset-Meldung in den nächsten sieben (7) Werktagen verschickt werden nach Durchlaufen dieses Prozesses aus Sicherheitsgründen.
Das Büro des Information Security halten diese aktualisiert werden, wenn Informationen sollten ändern, aber wir ermutigen alle Benutzer ihre Updates nach der erwarteten Veröffentlichung dieses Patch ausführen.

Genehmigt durch: Hans Pongratz,
Vizepräsident IT-Systeme & Dienstleistungen (CIO)

IT-Service Desk der Technischen Universität München!

IT-Sicherheit: zentrales Meldewesen (1/2)

IT-sicherheitsrelevante Vorfälle und Schwachstellen werden zentral dokumentiert und koordiniert, dazu gehören:

- Verlust von elektr. Geräten, auf denen sensible Daten gespeichert sind;
- Einbruch von Hackern in IT-Systeme der TUM;
- Verbreitung von Schadcode durch von der TUM betriebene IT-Systeme;
- Kompromittierung von Zugangsdaten;
- sicherheitskritische Schwachstellen bei im Einsatz befindlichen IT-Geräten und IT-Systemen.

➢ Abwicklung erfolgt über zentralen IT-Support (it-support@tum.de bzw. 289-17123)

IT-Sicherheit: zentrales Meldewesen (2/2)

- Flankierende Informationskampagne, um Sensibilität für IT-Sicherheit und IT-Sicherheitsbewusstsein zu fördern
- zentrale Hilfestellung zur Wiederherstellung des Betriebs nach einem sicherheitskritischen Vorfall
- CIO wird regelmäßig informiert, bei schwerwiegenden Fällen unverzüglich
- Bei Bedarf Einbindung von HSP, Datenschutzbeauftragten, Sicherheitsbeauftragten und Personalrat
- Neue Referentin IT-Sicherheit & Datenschutz im IT-Management des IT-Servicezentrums der TUM

Sicherheit

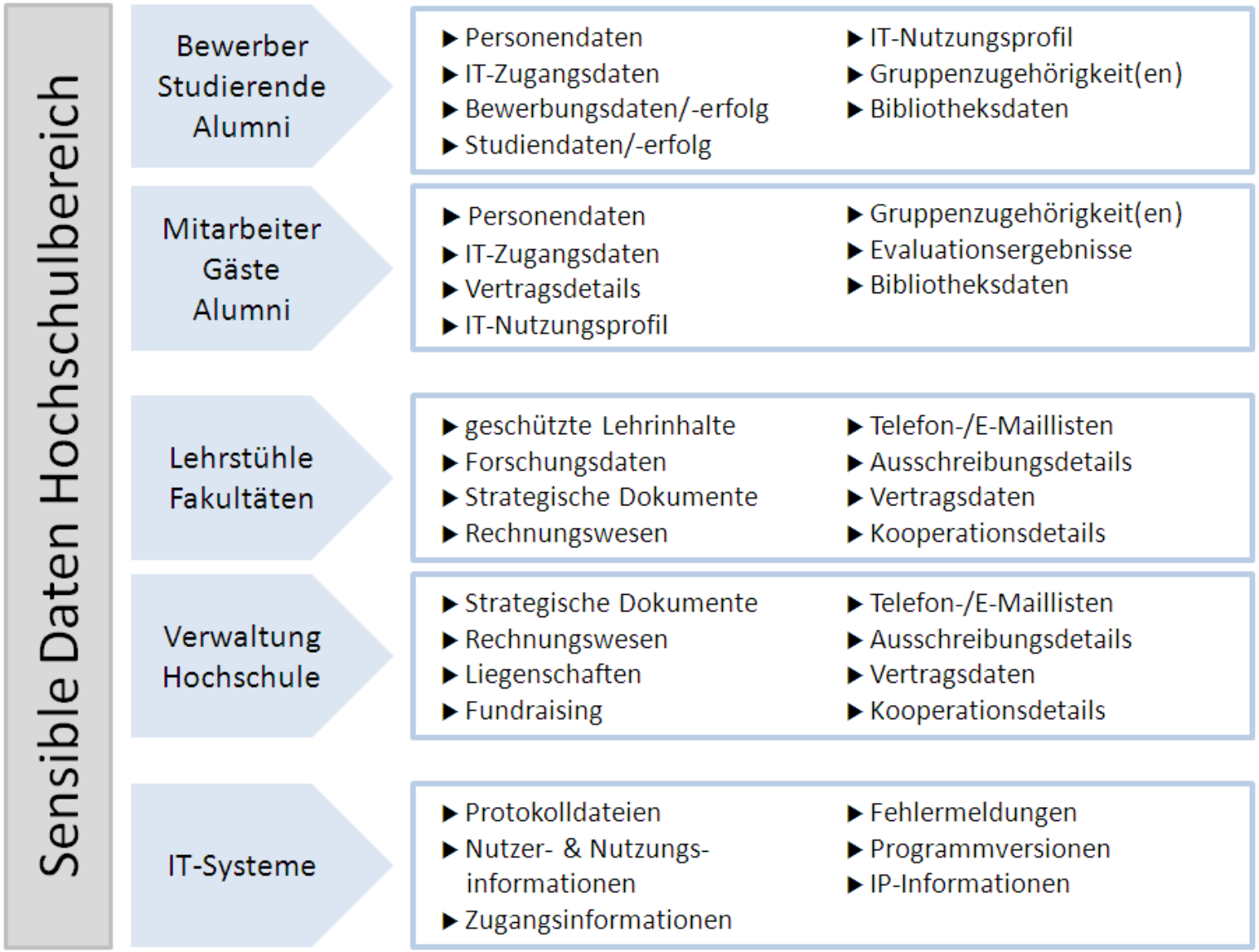
IT-Sicherheit

Grundwerte:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Beispiele für schützenswerte Daten im Hochschulumfeld:

- Bewerberinformationen
- Stammdaten
- Anmeldungs- und Prüfungsdaten
- Inhalte von Webseiten


Sensible Daten Hochschulbereich
Bewerber
Studierende
Alumni
▶ Personendaten
▶ IT-Zugangsdaten
▶ Bewerbungsdaten/-erfolg
▶ Studiendaten/-erfolg
▶ IT-Nutzungsprofil
▶ Gruppenzugehörigkeit(en)
▶ Bibliotheksdaten
Mitarbeiter
Gäste
Alumni
▶ Personendaten
▶ IT-Zugangsdaten
▶ Vertragsdetails
▶ IT-Nutzungsprofil
▶ Gruppenzugehörigkeit(en)
▶ Evaluationsergebnisse
▶ Bibliotheksdaten
Lehrstühle
Fakultäten
▶ geschützte Lehrinhalte
▶ Forschungsdaten
▶ Strategische Dokumente
▶ Rechnungswesen
▶ Telefon-/E-Maillisten
▶ Ausschreibungsdetails
▶ Vertragsdaten
▶ Kooperationsdetails
Verwaltung
Hochschule
▶ Strategische Dokumente
▶ Rechnungswesen
▶ Liegenschaften
▶ Fundraising
▶ Telefon-/E-Maillisten
▶ Ausschreibungsdetails
▶ Vertragsdaten
▶ Kooperationsdetails
IT-Systeme
▶ Protokolldateien
▶ Nutzer- & Nutzungs-informationen
▶ Zugangsinformationen
▶ Fehlermeldungen
▶ Programmversionen
▶ IP-Informationen

Datenschutz

- In Bayern geregelt durch BayDSG
- Datenschutzbeauftragter erteilt Verfahrensfreigaben und koordiniert über sein Sekretariat Auskunftsanfragen
- Datenschutzbevollmächtigte in Fakultäten und Einrichtungen
- Verfahrensverzeichnis
- Referentin für IT-Sicherheit & Datenschutz
- Regelmäßige Treffen mit Gesamtpersonalrat und CIO

IT-Compliance Brainstorming

- Wem & wie sollte IT-Vorfall gemeldet werden?
- IT-Benutzungsrichtlinien
- Social Media Policy
- Passwort-Policy
- Ausreichend Softwarelizenzen
- Urheberrecht
- Nutzung Cloud-Dienste
- Löschfristen
- Ausschreibungen
- Test IT-Sicherheit, u.a. Liegenschaftssicherheit
- …

Beispiel Checkliste

Themenbereich	Thema	geprüft
Archivierung	Konzept mit Aufbewahrungs- & Löschfristen	☐
	Revisionssicherheit	☐
	Wiederherstellung erfolgreich getestet	☐
Cloud-Dienste	Auftragsdatenvereinbarungsvertrag	☐
	Verfahrensfreigabe	☐
Dokumentation	Zugriff Systeme	☐
	Verfahrensverzeichnis	☐
	Prozesse	☐
Sicherheits-/Notfallkonzept	Backup	☐
	Raumzutritt	☐
	USV	☐
	Kommunikation	☐
…	…	

Erfolgsfaktoren

- Zur Organisation passendes Vorgehensmodell wählen (sukzessiv vs. großer Wurf)
- Aufwand für Mitglieder der Organisation darf nicht zu hoch sein
- Kommunikation & Change Management
- Steigerung Compliance Bewusstsein aller Mitglieder
- Compliance muss geübt & vorgelebt werden

Nichts ist einfacher als sich schwierig auszudrücken,
und nichts ist schwieriger als sich einfach auszudrücken.

Karl Heinrich Waggerl

Fragen?

-> pongratz@tum.de